



Design Basis Threat

Biosecurity Inspector Training

**Staten Serums Institut
31 August – 2 September 2009**

www.biosecurity.sandia.gov

SAND No. 2009-5485C

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.





The Role of Design Basis Threat in Laboratory Biosecurity



What is Design Basis Threat?

- **A DBT establishes the objectives of a facility security system**
 - Defines the assets to be protected
 - Defines the threats to protect those assets against
- **A DBT is necessary to ensure that security resources are used as efficiently as possible**
 - Ensures security system is designed for specific operations
 - **Security for biocontainment facilities should be different than an airport or bank**
 - Avoids blanket protection – protecting everything equally
 - **“Protect pencils like pencils, and diamonds like diamonds”**
 - Keeps the security experts in their lane
 - **Contractors will inevitably act in their own interest**
- **Critical that the DBT be set by policy – by the institution’s owners who are ultimately responsible for all of the institute’s operations and programs**
 - Only the institution’s owners can articulate the institution’s level of risk tolerance



DBT directly affects resources and operations

- **A DBT that reflects a highly risk averse management position**
 - i.e. many assets must be protected from many different threats
 - Security system may be very expensive to install, operate, and maintain
 - Security system may significantly infringe on the institute's operations

- **A DBT that reflects a highly risk tolerant management position**
 - i.e. few assets must be protected from few threats
 - Security system may be relatively inexpensive to install, operate, and maintain
 - Security system may have little impact on the institute's operations
 - Security system may have many vulnerabilities



Internal Pressures on DBT

- **Security inevitably affects the institution's operations**
 - Uses resources that could otherwise be directed elsewhere
 - Increases the cost of operations, costs that you must be able to pass on to your sponsors and customers
 - Will impact daily work of the staff – may make completing research more difficult, more expensive
 - May limit who can work in the institute, and when they can work
- **Security inevitably affects the institution's operations**
 - Institution's police
 - Emergency responders
 - Maintenance
 - Shipping
 - Procurement
 - Legal



External Pressures on DBT

- **What international, national, and/or local regulations specifically apply?**
 - BWC/UNSCR 1540 – general call to secure materials that could be used for developing a biological weapon
 - National regulations such as the US Select Agent Rule – it defines “select agents” as assets that must be protected, but it does not define what those agents must be protected against (“risk assessment”)
 - Are there any local regulations that must be incorporated into the DBT?
- **Perhaps the most important external consideration is political**
 - Can you defend your security posture to your sponsors, your community?
 - Imagine an interview with the media on this subject...
 - Imagine if something went wrong...can you defend yourself?



DBT as Policy

- **DBT attempts to resolve all of these thorny issues**
- **DBT should be developed by a select group of all relevant stakeholders**
 - Those who work in the labs: scientists, technicians, animal care givers, et al.
 - Those who work in the building: operations, maintenance, management, et al.
 - Those who work on the campus: administrators, Legal, et al.
- **DBT should become policy, signed by the highest authority possible**
 - That person who ultimately takes responsibility for all operations and programs at the institute – science, safety, security, etc.
 - That person who ultimately controls the resources for the institute
 - That person who ultimately will be accountable if something goes wrong
- **DBT will be sensitive information, and should be protected accordingly**



How should the DBT be used?

- **DBT should be given to team responsible for conducting the site security risk assessment or vulnerability assessment**
- **Tasking should be for the security risk assessment team to evaluate the institution against the objectives specified in the DBT**
 - What is the relative risk of the various defined threats attacking the various defined assets?
 - Does the current security system appropriately focus on the defined security scenarios that are highest risk?
 - Are security resources proportionally allocated to mitigate the highest risks?
 - What vulnerabilities exist that need to be corrected? (unacceptable risk)
 - What vulnerabilities exist that do not need to be corrected? (acceptable risk)



Following the site security risk assessment

- **The institution should use the risk assessment results to determine whether or how the existing security system should be modified or improved**
- **After any necessary modifications, the institution should have a security system that meets all the objectives of the DBT, and also prioritizes security against the highest risk security scenarios**
- **Then, the institution should write a laboratory biosecurity plan that reflects the full operation of the resulting security system**
- **The security plan should reference the site risk assessment, and the site risk assessment should reference the DBT**
 - Combined, all three documents will help ensure an effective and efficient security system, and should satisfy any external auditors



Establishing a DBT – defining assets

- **The easy part....**
- **Define the assets that should be protected at the institution**
 - Dangerous pathogens
 - Other pathogens
 - Specific equipment
 - Specific facilities
 - Specific information
 - Etc.



Establishing a DBT – defining threats

- **The hard part...**
 - Little information about terrorists' interest in biological weapons, or their methods for acquiring them
 - Few bioscience facilities have been attacked by adversaries
 - Little to no information available about the targeting of bioscience facilities
 - But...it happens
- **Define the threats that the defined assets should be protected against**
 - **Insiders**
 - **Scientists/technicians/animal care givers**
 - **Operations and maintenance personnel/administrative personnel**
 - **Visitors**
 - **Etc.**
 - **Outsiders**
 - **Individuals**
 - **Animal rights groups**
 - **Terrorist groups**
 - **Etc.**



Establishing a DBT – defining scenarios

- Last step is to combine the assets and threats into credible scenarios that the institution's security system should protect against



Exercise: Creating a Design Basis Threat



Class Exercise

- **Asset:**
- **Adversaries**
- **Scenarios**



Class Exercise

- **Asset:**
- **Adversaries**
- **Scenarios**



Discussion:

Where to get Information for DBT?

- **Assets**
- **Adversaries**
- **What are appropriate scenarios?**



Review of Historical Threats to Biocontainment Facilities



Historical Security Risks to Biocontainment Laboratories

- Theft of pathogens
- Attacks by animal rights extremists
- Theft of intellectual property
- Theft of property
- Regulatory risks



Theft of Pathogens

- **26 terrorist and criminal incidents with biological materials originating from laboratories**
- **Limited evidence of attacks on bioscience facilities by outside adversaries with the intent to steal pathogens**
 - Only one recent example in the open literature—an attempted theft at the central reference laboratory for animal health in Indonesia targeted their pathogen collection, and was thwarted by a security system recently installed by the US government
- **In contrast, there are many examples of people who work at bioscience facilities taking pathogens or toxins with the intent to commit malicious acts. For example,**
 - Mitsuru Suzuki—*Shigella dysenteriae* and *Salmonella typhi*, 1964-1966
 - Diane Thompson—*Shigella dysenteriae* Type 2, Oct 1996





Attacks by Animal Rights Extremists

- **At least 250 animal rights movement groups in the United States**
- **Significant escalation of violence since 2000**
- **Illustrative examples**
 - Arson/sabotage
 - 1987: ALF arson attack on UC Davis Animal Diagnostics Laboratory
 - Damages: \$5.1 million, 1 building and 20 vehicles destroyed
 - 1989: ALF sabotage of Texas Tech University
 - Damages: \$700,000, destroyed records and computers
 - 2002: ELF arson of University of Minnesota's Microbial and Plant Genomics Research Center while building was under construction
 - Damages: \$250,000
 - Theft of animals
 - 1987: Band of Mercy theft of infected cats from Beltsville Agricultural Research Center
 - 2005: ALF stole 10 – 21 mice and vandalized lab at Louisiana State University School of Veterinary Medicine

Theft of Intellectual Property

- **Illustrative examples**

- Two former post-docs at Harvard Medical School indicted by grand jury for theft of research materials
 - Shipped 20 boxes of materials related to drug discovery research to new employer in Texas
- Post-doc at Cornell arrested with >250 test tubes, vials, and petri dishes in luggage before boarding a flight to Shanghai
 - Bacteria and yeast cultures for commercial enzyme production





Theft of General Property

- **Illustrative examples**

- Former computer systems administrator for the Naval Research laboratory stole ~19,000 pieces of computer and office equipment over a ten year time period
- Theft of \$86,000 worth of copper (reels of used cable, copper blocks) from Brookhaven National Laboratory



Regulatory Risks

- Substantive financial and penal penalties are possible for running afoul of security regulations
- There can also be substantive negative impacts to a facility's operations
- Illustrative examples
 - Texas A&M - \$1 million fine for select agent regulatory violations; also had work halted
 - Prof. Thomas Butler was convicted on 47 counts related to missing vials of plague





Example Design Basis Threat



Assets Could Include

- **Regulated agents (higher risk, lower risk categories)**
- **Other pathogens (higher risk, lower risk categories)**
- **Strain collections**
- **Unique reagents**
- **Animals**
 - Infected animals
 - Clean animal colonies
- **Information**
 - Proprietary, Sensitive But Unclassified, Classified
- **Specialized equipment**
- **General property**
- **Mission critical support facilities**
 - Such as: containment laboratories or back-up generators
- **Non mission critical facilities**



Defining Threats

- **Details about the insider**
 - Is he/she acting overtly or covertly?
 - Is he/she acting alone?
 - Is he/she coerced into acting?

- **Details about the outsiders**
 - How many?
 - Institute knowledge?
 - System knowledge?
 - Willing to commit violence?
 - Willing to commit suicide?
 - What tools would the outsider use?
 - Vehicle bomb
 - Package bomb
 - Weapons



Insiders

- **Insider**

- A person who has official business with the institute, and who has authorized access.

- **Categories**

- Employee with varying levels of access to the institute
 - Full access to the room where asset is located
 - Building access
 - Site access
- Visitor with varying levels of access to the institute
 - Full access to the room where asset is located
 - Building access
 - Site access



Insider Examples:

- **Scientist, Technician, etc.**

- One person
- Acts covertly
- Non violent (violence not necessary)
- With system knowledge that can be used to his/her advantage
- Can access facility, assets, and/or physical protection system without raising alarm or suspicion of others
- Will choose best time to commit an act; wants to avoid being caught

- **Visitor**

- Visiting researcher, conference/meeting participants, maintenance personnel, etc.
- Single person
- Acts covertly
- Non violent (violence not necessary)
- May have partial system knowledge that can be used to his/her advantage
- May have access to facility, assets, and/or physical protection system without raising alarm or suspicion of others
- Will choose best time to commit an act; wants to avoid being caught



Outsiders

- **Outsider**
 - A person or group who does not have official business with the institute, and does not have authorized access to the institute.
- **Categories of outsiders include**
 - Single terrorist
 - Terrorist groups
 - Extremist group
 - Criminal
 - Vandal
- **Collusion**
 - Combination of an Insider working with an Outsider



Outsiders: Terrorists

- **Terrorist groups**
 - Acts overtly
 - Usually well funded, well equipped, and trained
 - May have specific tools, such as explosives and weapons
 - Assumed to be violent and may be willing to die
 - None to minimal system knowledge (only publicly available information)
- **Single terrorist**
 - Acts overtly (unless he becomes an Insider)
 - May be moderately funded, equipped, and trained
 - May have specific tools, such as explosives and weapons (but can carry and use less than a group)
 - Assumed to be violent and may be willing to die
 - None to minimal system knowledge (only publicly available information)



Outsider: Other Examples

- **Extremist Groups**

- Animal rights movements, anti-GMO groups, etc.
- Groups of varying size
- Acts overtly
- Objective is to seek political gain through sabotage and financial damage; may also seek to release animals
- May resort to violence but generally not willing to die
- None to minimal system knowledge (only publicly available information)

- **Criminals**

- One person
- Acts overtly (unless he becomes an Insider)
- May use weapons and hand tools
- Unlikely to be violent, not willing to die
- Objective is financial gain
- None to minimal system knowledge (only publicly available information)
- Could be affiliated with organized crime in extreme cases



Example DBT (1)

- **Asset: Higher risk regulated pathogens**
- **Adversaries**
 - Employee with full access
 - Employee with building access
 - Employee with site access
 - Visitor with full access
 - Visitor with building access
 - Visitor with site access
 - Single terrorist
 - Terrorist group
- **Scenarios**
 - Adversary overtly or covertly steals agent to later use maliciously in an act of bioterrorism, or to commit a biocrime



Example DBT (2)

- **Asset: Lower risk select agents**
- **Adversaries**
 - Employee with full access
 - Employee with building access
 - Employee with site access
 - Visitor with full access
 - Visitor with building access
 - Visitor with site access
 - Single terrorist
- **Scenarios**
 - Adversary overtly or covertly steals agent to later use maliciously in an act of bioterrorism, or to commit a biocrime



Example DBT (3)

- **Asset: Unique reagents**
- **Adversaries**
 - Employee with full access
 - Employee with building access
 - Employee with site access
 - Visitor with full access
 - Visitor with building access
 - Visitor with site access
- **Scenarios**
 - Adversary covertly steals agent for competitive gain or as part of foreign intelligence efforts
 - Adversary sabotages collection to disrupt mission



Example DBT (4)

- **Asset: Information**
- **Adversaries**
 - Employee with full access
 - Employee with building access
 - Employee with site access
 - Visitor with full access
 - Visitor with building access
 - Visitor with site access
 - Single terrorist (cyber)
 - Terrorist group (cyber)
 - Extremist (cyber)
 - Vandal (cyber)
- **Scenarios**
 - Adversary covertly steals information for competitive gain or as part of foreign intelligence efforts
 - Adversary steals operation-specific information to facilitate a later attack
 - **e.g. Insider collusion with terrorist group**
 - Adversary steals information for political gain
 - Adversary sabotages electronic data for unknown reasons



Example DBT (5)

- **Asset: Specialized equipment**
- **Adversaries**
 - Employee with full access
 - Employee with building access
 - Employee with site access
 - Visitor with full access
 - Visitor with building access
 - Visitor with site access
- **Scenarios**
 - Adversary sabotages equipment to disrupt mission



Example DBT (6)

- **Asset: Mission critical support facilities**
- **Adversaries**
 - Employee with full access
 - Employee with building access
 - Employee with site access
 - Visitor with full access
 - Visitor with building access
 - Visitor with site access
 - Terrorist group
 - Single terrorist
 - Extremists
- **Scenarios**
 - Adversaries seek to destroy facility to disrupt mission or make a political statement with vehicle bomb, arson
 - Adversaries sabotage facility to disrupt mission or make a political statement (damage facilities or injure/kill site personnel) by package bomb, arson
 - Adversaries sabotage building automation system to disrupt mission or make a political statement by cyber attack
 - Adversaries sabotage security system (e.g. by cyber attack) to facilitate future assault